Insider Threats in the Software Development Lifecycle

CERT® Insider Threat Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Randy Trzeciak
Dan Costa
05 November 2014

Software Engineering Institute | **Carnegie Mellon University**

			Form Approved OMB No. 0704-0188	

Report Documentation Page

1. REPORT DATE **05 NOV 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Insider Threats in the SDLC**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Randy Trzeciak Daniel Costa**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES **The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **32**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Agenda

The Insider Threat Center at CERT

Types of Insider Incidents

Insider Threat Issues in the SDLC

– Case Studies

Mitigation Strategies

CERT Insider Threat Resources

THE INSIDER THREAT CENTER AT CERT

What is the CERT Insider Threat Center?

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Our mission: *The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.*

Software Engineering Institute | **Carnegie Mellon University**

Goal for an Insider Threat Program
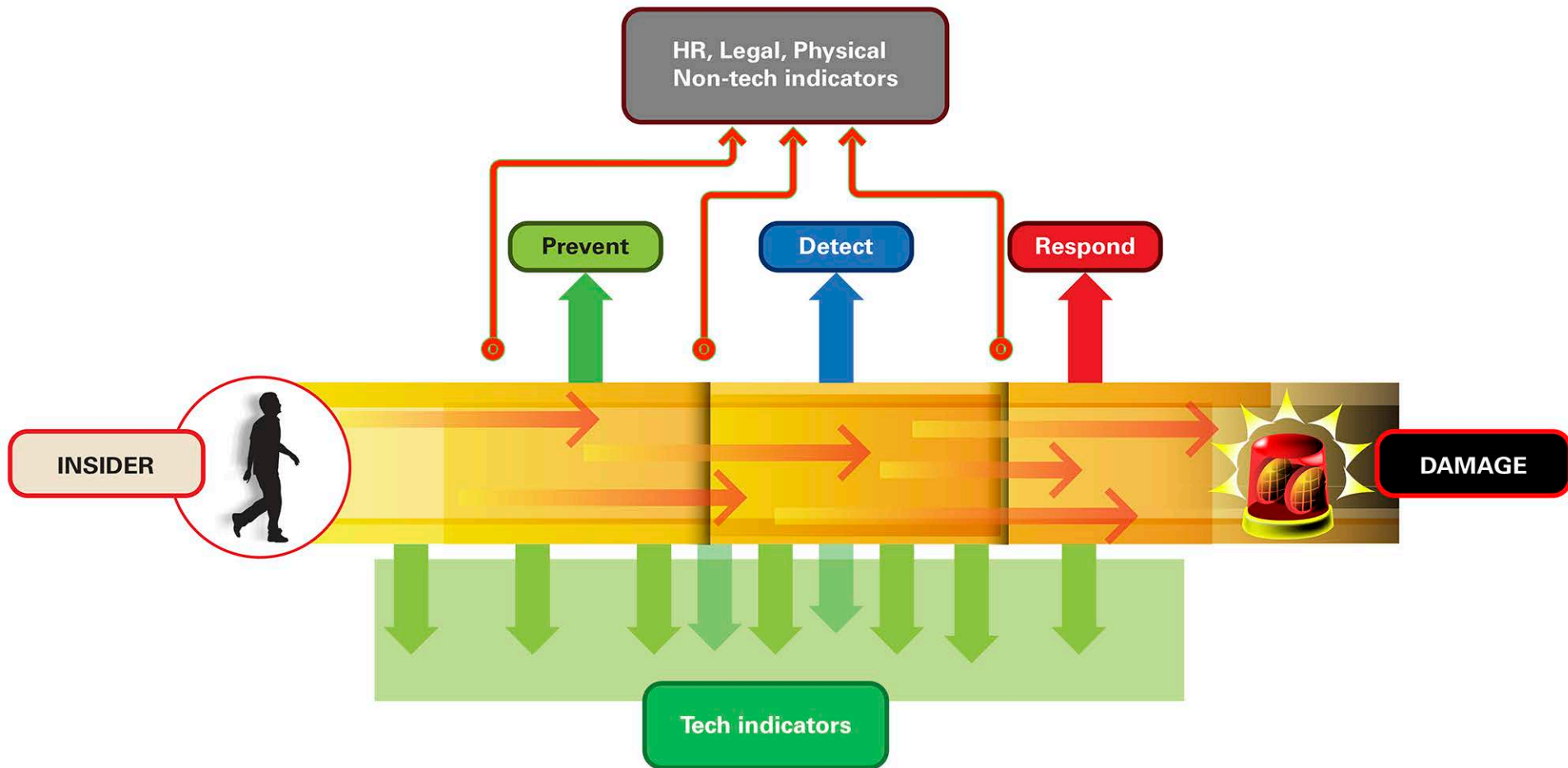
Opportunities for prevention, detection, and response for an insider incident

CERT's Unique Approach to the Problem

Research Models
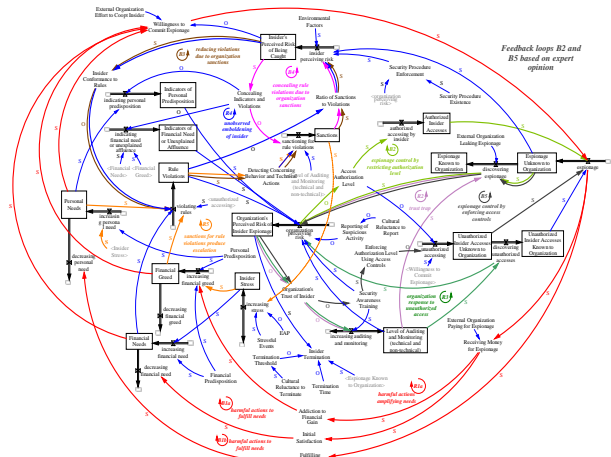
Deriving Candidate Controls and Indicators
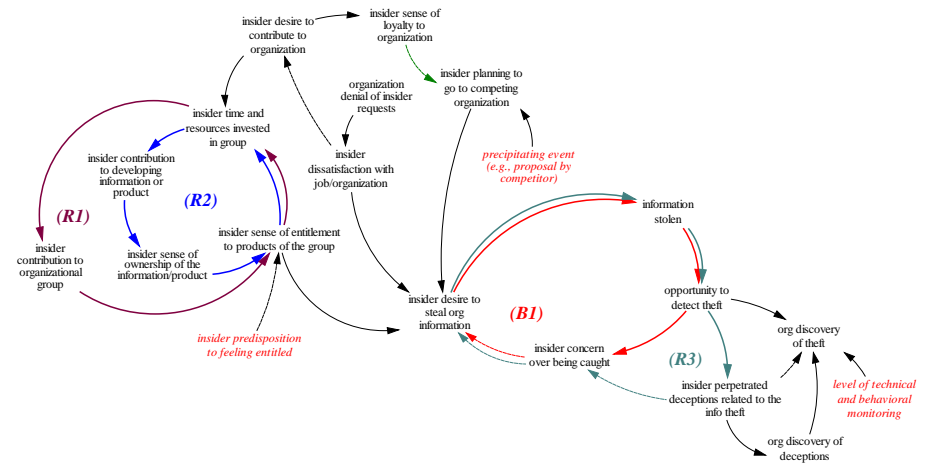
Our lab transforms that into this…

```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was
disabled. *" | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat
Account_Name "@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000
AND recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip,
sender_address, recipient_address, message_subject, total_bytes'
```

What is a Malicious Insider Threat?

Current or former employee, contractor, or other business partner who

- has or had authorized access to an organization's network, system or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

What is an Unintentional Insider Threat?

Current or former employee, contractor, or other business partner who

- has or had authorized access to an organization's network, system, or data and who, through
- their action/inaction without malicious intent
- cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

Insider Threat

9

CERT's Insider Threat Case Database

U.S. Crimes by Category

TYPES OF INSIDER INCIDENTS

Software Engineering Institute | **Carnegie Mellon University**
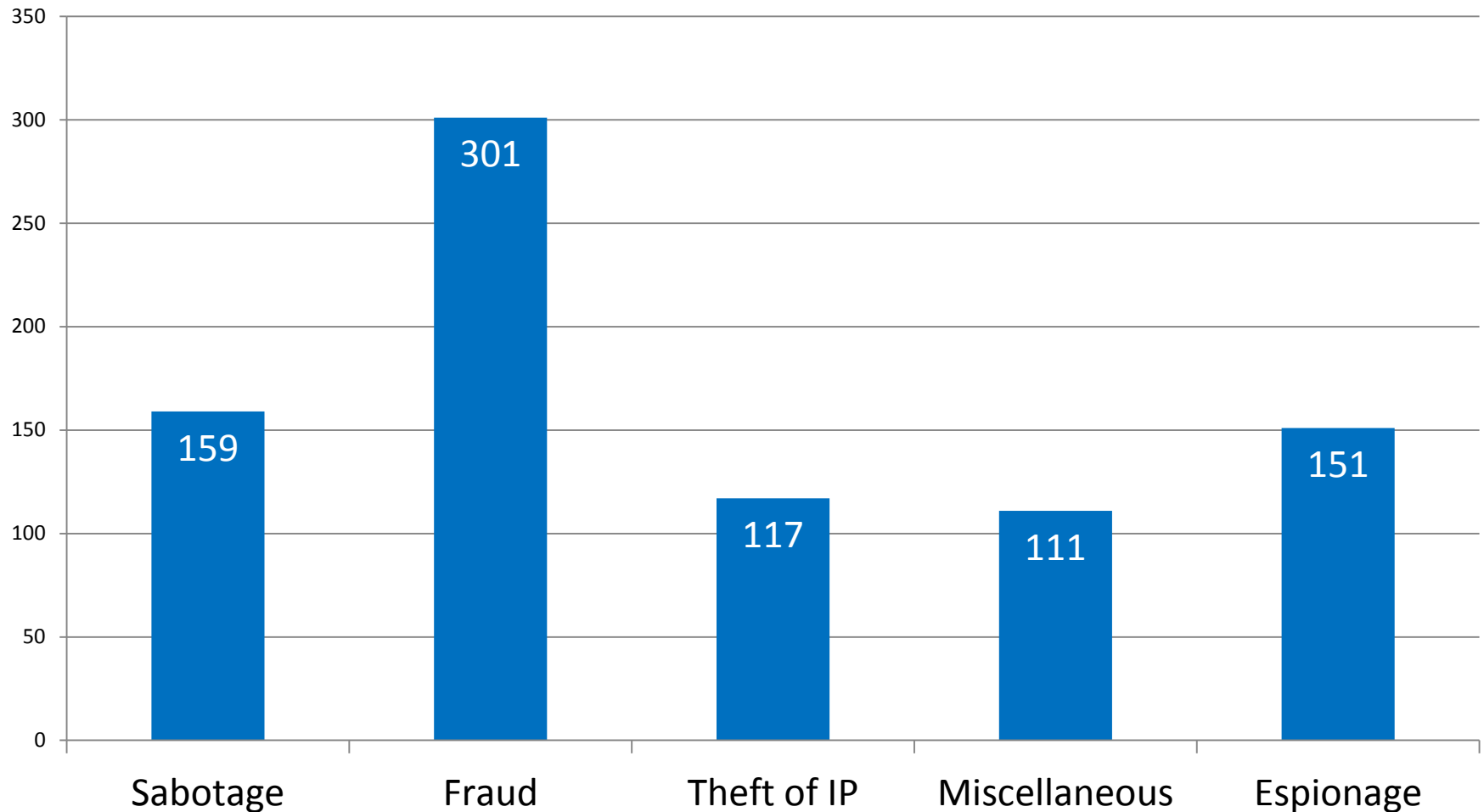
The Insider Threat

There is not one "type" of insider threat

- Threat is to an organization's critical assets
  - People
  - Information
  - Technology
  - Facilities
- Based on the motive(s) of the insider
- Impact is to Confidentiality, Availability, Integrity

There is not one solution for addressing the insider threat

- Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider

Separate the "Actor" from the "Target" from the "Impact"

Actor(s)	Target	Impact
Employees • Current • Former Contractors Subcontractors Suppliers Trusted Business Partners	Critical Assets • People • Technology • Information • Facilities	Confidentiality Availability Integrity
WHO	**WHAT**	**HOW**

Types of Insider Incidents

Insider IT sabotage
An insider's use of IT to direct specific harm at an organization or an individual.
Insider theft of intellectual property (IP)
An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.
Insider fraud
An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).
National Security Espionage
The act of stealing and delivering, or attempting to deliver, information pertaining to the national defense of the United States to agents or subjects of foreign countries, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation.

Summary of Insider Incidents

	IT Sabotage	Fraud	Theft of Intellectual Property
Current or former Employee?	Former	Current	Current (within 30 days of resignation)
Type of position	Technical (e.g. sys admins, programmers, DBAs)	Non-technical (e.g. data entry, customer service) or their managers	Technical (e.g. scientists, programmers, engineers) or sales
Gender	Male	Fairly equally split between male and female	Male
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) or Customer Information
Access Used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At Work

INSIDER THREATS IN THE SDLC

Insider Threat Issues in the SDLC

"those aspects of an organization's software development or maintenance policies and processes that insiders exploited to carry out their attack"

- Cappelli, D., Moore, A. & Trzeciak, R. (2012). The CERT Guide to Insider Threats : How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley.
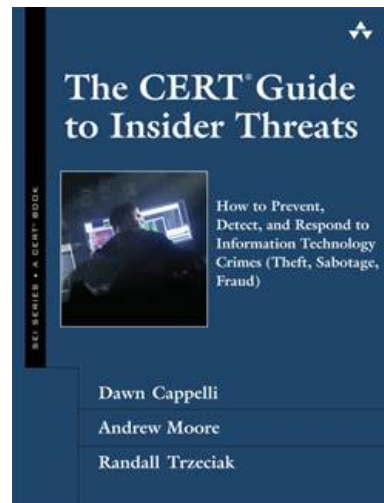
Phases of the Life Cycle Exploited

Requirements / Design

System Implementation

System Verification

Operations and Maintenance

Requirements / Design Exploits

Neglecting to define **authentication** and **role-based access control** requirements simplified insider attacks.

Neglecting to define **security requirements / separation of duties for automated business processes** provided an easy method for insider attack.

Neglecting to define requirements for **automated data integrity checks** gave insiders the security of knowing their actions would not be detected.

Neglecting to consider security vulnerabilities posed by **authorized system overrides** resulted in an easy method for insiders to "get around the rules".

System Implementation Exploits

Lack of **code reviews** and inadequate **software documentation** have
- Facilitated insertion of backdoors and logic bombs into source code
- Allowed intentionally obfuscated code to be added to production systems

Insufficient attention to details in **automated workflow processes** enabled insiders to commit malicious activity.

Inability to **attribute actions** to a single user enabled a project leader to sabotage his team's development project.

System Verification Exploits

Insufficient **separation of duties** facilitated insider crimes.

- Malicious insiders employed as software testers have made unauthorized modifications to source code that they later exploited in production

Poor **requirements traceability** allowed security vulnerabilities that were addressed in the requirements and design phase but not properly implemented to go undetected.

Inadequate **software test coverage** can lead to detectable security vulnerabilities being released into production systems.

Operations and Maintenance Exploits

Lack of enforcement of **documentation practices** and **backup procedures** prohibited recovery efforts when an insider deleted the only copy of source code for a production system.

Use of the same **password file** for development and operations enabled insiders to access and steal sensitive data from operational systems

Unrestricted access to all customers' systems enabled a computer technician to plan a virus directly on customer networks

Lack of **configuration control** and well-defined **business processes** enabled libelous material to be published to organizations' websites.

Operations and Maintenance Exploits (contd.)

Lack of **code reviews** and ineffective **configuration control** processes facilitated insertion of malicious code into production.

Ineffective or lack of **backup processes** amplified the impact of mass data deletion.

End-user access to source code for systems they used enabled modification of security measures built into the source code.

Inadequate **issue tracking** procedures led to insiders exploiting system vulnerabilities they had previously reported.

MITIGATION STRATEGIES

Insider Threats in the SDLC
Randy Trzeciak, Dan Costa, 05 November 2014
© 2014 Carnegie Mellon University

24

Mitigation Strategies

Design and build a system architecture that allows for efficient recovery or sustains the organization during disasters

Utilize configuration and access control for source code and production data

Deploy a formal code review process to prevent malicious code from being inserted into production systems

Create and enforce authorization and approval steps in automated workflow to ensure proper approvals for critical business functions
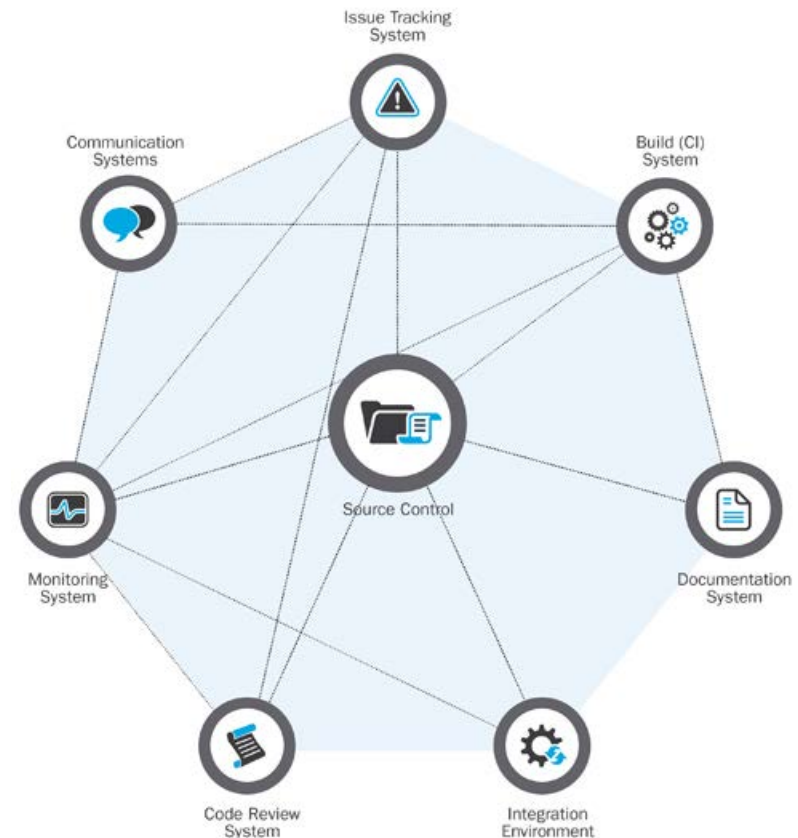
Full traceability from requirements to verification to prevent unauthorized functionality from inclusion in production systems

DevOps as an Insider Threat Control

Integration of many development and operations processes provides opportunities for effective insider threat controls

- Source code changes can be traced to appropriate issue tracking system items and verified by another party
- Build systems can be configured to ensure all integration and unit tests are passed prior to generating a new deployment-ready system
- Monitoring systems can be configured to notify team members when suspicious activity is detected

Source: "A Generalized Model for Automated DevOps", C. Aaron Cois, http://blog.sei.cmu.edu/post.cfm/generalized-model-automated-devops-153

http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

COMMON SENSE GUIDE TO MITIGATING INSIDER THREATS

CERT Common Sense Guide to Mitigating Insider Threats – Recommended Best Practices

Consider threats from insiders and business partners in enterprise-wide risk assessments.	Institutionalize system change controls.
Clearly document and consistently enforce policies and controls.	Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
Incorporate insider threat awareness into periodic security training for all employees.	Monitor and control remote access from all end points, including mobile devices.
Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	Develop a comprehensive employee termination procedure.
Anticipate and manage negative issues in the work environment.	Implement secure backup and recovery processes.
Know your assets.	Develop a formalized insider threat program.
Implement strict password and account management policies and practices.	Establish a baseline of normal network device behavior.
Enforce separation of duties and least privilege.	Be especially vigilant regarding social media.
Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	Close the doors to unauthorized data exfiltration.
Institute stringent access controls and monitoring policies on privileged users.	

CERT INSIDER THREAT RESOURCES

CERT Insider Threat Resources

Insider threat awareness training

Insider threat certificate programs

- Insider Threat Program Manager
- Insider Threat Vulnerability Assessor
- Insider Threat Program Evaluator

Insider threat vulnerability assessments

Insider threat program evaluations

www.cert.org/insider-threat

- Technical reports
- Insider threat technical controls
- Insider threat blog

DISCUSSION

Insider Threats in the SDLC
Randy Trzeciak, Dan Costa, 05 November 2014   **31**
© 2014 Carnegie Mellon University

Contact Information

Randy Trzeciak

Technical Manager

CERT Insider Threat Center

Telephone: +1 412-268-5800

Email: insider-threat-feedback@cert.org

Web

www.cert.org/insider-threat

www.sei.cmu.edu

Dan Costa

Member of the Technical Staff

CERT Insider Threat Center

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257